ABSTRACT OF THE DISCLOSURE

A malware detection system that determines whether an executable code module is malware according to behaviors exhibited while executing is presented. The malware detection system determines the type of code module and executes the code module in a behavior evaluation module for evaluating code corresponding to the code module's type. Some behaviors exhibited by the code module, while executing in the behavior evaluation module, are recorded as the code module's behavior signature. After the code module has completed its execution, the code module's behavior signature is compared against known malware behavior signatures stored in a malware behavior signature store. A determination as to whether the code module is malware is based on the results of the comparison.